

Nathan R. Ring
Nevada State Bar No. 12078
STRANCH, JENNINGS & GARVEY, PLLC
3100 W. Charleston Boulevard, Suite 208
Las Vegas, NV 89102
Telephone: (725) 235-9750
lasvegas@stranchlaw.com

Jeff Ostrow (*pro hac vice* forthcoming)
Ken Grunfeld (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, Florida 33301
Telephone: 954-525-4100
ostrow@kolawyers.com
grunfeld@kolawyers.com

Counsel for Plaintiff and the Proposed Class

**UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA**

NEIL LEVITT, individually and on behalf of all
others similarly situated,

Plaintiff,

v.

NORTHWELL HEALTH, INC. and PERRY
JOHNSON & ASSOCIATES, INC.,

Defendants.

Case No. 2:23-cv-1892

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Neil Levitt, individually and on behalf of all similarly situated persons, alleges the following against Northwell Health, Inc. (“Northwell”) and Perry Johnson & Associates, Inc. (“PJ&A”) (collectively, “Defendants”), upon personal knowledge as to his own actions, and, *inter alia*, his counsels’ investigation and upon information and belief as to all other matters:

I. NATURE OF THE ACTION

1. This class action arises out of the cyberattack and data breach that occurred between around March 27, 2023 and May 2, 2023 (“Data Breach”) resulting from Defendants’ failure to implement reasonable and industry standard data security practices.

2. Northwell is New York State’s largest healthcare provider, with hospitals in New York City, Long Island, and Westchester, including North Shore University Hospital and Long Island Jewish Medical Center. It has more than 900 hospitals and care centers, more than 85,000 employees, and more than 2 million patients per year.¹ In the course of providing its healthcare services, Northwell collected and maintained certain personally identifiable information of Plaintiff and the putative Class Members (defined in the Class Definition section, *infra*).

3. PJ&A is a medical transcription services that provides customized transcription solutions and coding, billing, recording, digital dictation, and court reporting services.²

4. Plaintiff’s and Class Members’ sensitive personal information—which they entrusted to Defendants on the mutual understanding that Defendants would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

5. The Private Information compromised in the Data Breach included Plaintiff’s and Class Members’ names, Social Security numbers, dates of birth, addresses, medical record numbers, and hospital account numbers (“personally identifiable information” or “PII”), and clinical information including the name of the treatment facility, name of healthcare provider, admission diagnosis, date(s) and time(s) of service, and files containing transcripts of operative reports, consult reports, history and physical exams, and discharge summaries or progress results (which may include

¹ <https://northwell.edu/about-northwell> (last visited Nov. 15, 2023).

² *Perry Johnson & Associates, Inc.*, BLOOMBERG, <https://www.bloomberg.com/profile/company/0212500D:US#xj4y7vzkg> (last visited Nov. 15, 2023).

1 diagnoses, testing results, medical history, family medical history, surgical history, social history,
2 medications, allergies and other observational information), which is all protected health information
3 as defined by the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) (“PHI,”
4 and collectively with PII, “Private Information”).

5
6 6. The Private Information compromised in the Data Breach was exfiltrated by cyber-
7 criminals and remains in the hands of those cyber-criminals who targeted Private Information for its
8 value to identity thieves.

9 7. As a result of the Data Breach, Plaintiff and approximately 3,891,565 Class
10 Members,³ suffered concrete injuries in fact including, but not limited to: (i) Plaintiff's Private
11 Information being disseminated on the dark web; (ii) Plaintiff experiencing an increase in spam calls,
12 texts, and/or emails; (iii) lost or diminished value of their Private Information; (iv) lost opportunity
13 costs associated with attempting to mitigate the actual consequences of the Data Breach, including
14 but not limited to lost time; (v) invasion of privacy; (vi) loss of benefit of the bargain; and (vii) the
15 continued and certainly increased risk to their Private Information, which: (a) remains unencrypted
16 and available for unauthorized third parties to access and abuse; and (b) remains backed up in
17 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails
18 to undertake appropriate and adequate measures to protect the Private Information.
19

20
21 8. The Data Breach was a direct result of Defendants' failure to implement adequate and
22 reasonable cyber-security procedures and protocols necessary to protect its clients' patients' Private
23 Information from a foreseeable and preventable cyber-attack.
24
25
26

27 ³ “According to News12 Long Island, Northwell Health initially released a draft statement indicating
28 3,891,565 individuals had been affected, although the statement was later recalled and Northwell
Health said it was unable to confirm exactly how many individuals had been affected.”
<https://www.hipaajournal.com/northwell-health-pja-data-breach/> (last visited Nov. 15, 2023).

1 9. Defendants maintained the Private Information in a reckless manner. In particular,
2 the Private Information was maintained on Defendants' computer network in a condition vulnerable
3 to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for
4 improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to
5 Defendants, and thus, Defendants were on notice that failing to take steps necessary to secure the
6 Private Information from those risks left that property in a dangerous condition.

7
8 10. Defendants disregarded the rights of Plaintiff and Class Members by, *inter alia*,
9 intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures
10 to ensure its data systems were protected against unauthorized intrusions; failing to disclose that they
11 did not have adequately robust computer systems and security practices to safeguard Class Members'
12 Private Information; failing to take standard and reasonably available steps to prevent the Data
13 Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data
14 Breach.

15
16 11. Plaintiff's and Class Members' identities are now at risk because of Defendants'
17 negligent conduct because the Private Information that Defendants collected and maintained is now
18 in the hands of data thieves.

19
20 12. Armed with the Private Information accessed in the Data Breach, data thieves have
21 already engaged in identity theft and fraud and can in the future commit a variety of crimes including,
22 e.g., opening new financial accounts in Class Members' names, taking out loans in Class Members'
23 names, using Class Members' information to obtain government benefits, filing fraudulent tax
24 returns using Class Members' information,, and giving false information to police during an arrest.

25 13. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a
26 heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and
27 in the future closely monitor their financial accounts to guard against identity theft.
28

15. Plaintiff brings this class action lawsuit on behalf all those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

17. Plaintiff seeks remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

18. Plaintiff Neil Levitt is a natural person and citizen of the State of New York, and received a notice letter from Defendants dated November 3, 2023.

20. PJ&A is a corporation organized under the laws of Nevada with its principal place of business located at 1489 W. Warm Springs Rd., Suite 110, Henderson, NV 89012.

21. The Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5 million, exclusive of interest and costs. The number of class members is over 100, many of whom reside outside the State

1 of Nevada and who have different citizenship from at least one of the Defendants. Thus, minimal
 2 diversity exists under 28 U.S.C. §1332(d)(2)(A)

3 22. This Court has jurisdiction over Defendants because at least one of the Defendants
 4 is domiciled in this District and both operate in this District.

5 23. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because at least
 6 one of the Defendants' principal place of business is located in this District, a substantial part of the
 7 events giving rise to this action occurred in this District, and Defendants have harmed Class
 8 Members as a result of actions that have occurred in this District.

9 IV. FACTUAL ALLEGATIONS

10 A. *Defendants' Business and The Data Breach*

11 24. Northwell is the largest provider of healthcare in New York State, encompassing 21
 12 hospitals and 890 outpatient facilities in all five boroughs of New York City, Long Island, and
 13 Westchester.⁴

14 25. In the course of the patient-provider relationship, patients, including Plaintiff and
 15 Class Members, provided Defendants with at least the following information: names, Social Security
 16 numbers, dates of birth, addresses, medical record numbers, hospital account numbers, and the full
 17 range of diagnosis and treatment information, recorded through PG&A's medical transcription
 18 services.

19 26. In the Notice of Data Breach letters sent to Plaintiff and Class Members (the "Notice
 20 Letter"), Defendants admit that "PJ&A became aware of a data security incident impacting our
 21 systems on May 2, 2023."⁵

22
 23
 24
 25
 26
 27
 28 ⁴ <https://northwell.edu/about-northwell> (last visited Nov. 15, 2023).

⁵ Ex. A (Notice Letter).

1 27. Omitted from the Notice Letter were the root cause of the Data Breach, the
2 vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not
3 occur again. To date, these omitted details have not been explained or clarified to Plaintiff and Class
4 Members, who retain a vested interest in ensuring that their Private Information remains protected.

5 28. Upon information and belief, the cyberattack was targeted at Defendants, due to its
6 status as a healthcare entity service provider that collects, creates, and maintains Private Information
7 on its computer networks and/or systems.

8 29. As Defendants' Notice Letter admits, Plaintiff's and Class Members' Private
9 Information was, in fact, compromised and acquired in the Data Breach.

10 30. Because of this targeted cyberattack, data thieves were able to gain access to and
11 obtain data from Defendants that included the Private Information of Plaintiff and Class Members.

12 31. As evidenced by the Data Breach, the Private Information contained in Defendants'
13 network was not encrypted. Had the information been properly encrypted, the data thieves would
14 have exfiltrated only unintelligible data.

15 32. Plaintiff's Private Information was accessed and stolen in the Data Breach and
16 Plaintiff has come to learn that his stolen Private Information is currently available for sale on the
17 dark web following the Data Breach.

18 33. Plaintiff has also experienced an increased number of spam and suspicious messages
19 following the Data Breach and believes that these may be phishing attempts designed to gain access
20 to additional personal information.

21 34. Due to the actual and imminent risk of identity theft as a result of the Data Breach,
22 Plaintiff and Class Members must, as Defendants' Notice Letter encourages, monitor their financial
23 accounts for many years to mitigate the risk of identity theft.

24 35. In the Notice Letter, Defendants makes an offer of 12 months of credit monitoring
25 services through Equifax. This is wholly inadequate to compensate Plaintiff and Class Members as
26
27
28

1 it fails to provide for the fact that victims of data breaches and other unauthorized disclosures
2 commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely
3 fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and
4 Class Members' Private Information.

5
6 36. That Defendants is encouraging victims of the Data Breach to enroll in credit
7 monitoring and identity theft restoration services is an acknowledgment that the impacted
8 individuals' Private Information was acquired, thereby subjecting Plaintiff and Class Members to a
9 substantial and imminent threat of fraud and identity theft.

10 37. Defendants had obligations created by the FTC Act, HIPAA, contract, state and
11 federal law, common law, and industry standards to keep Plaintiff's and Class Members' Private
12 Information confidential and to protect it from unauthorized access and disclosure.

13
14 **B. Data Breaches Are Preventable**

15 38. Defendants could have prevented this Data Breach by, among other things, properly
16 encrypting or otherwise protecting their equipment and computer files containing Private
17 Information.

18 39. Defendants did not use reasonable security procedures and practices appropriate to
19 the nature of the sensitive information they were maintaining for Plaintiff and Class Members,
20 causing the exposure of Private Information, such as encrypting the information or deleting it when
21 it is no longer needed.

22
23 40. The unencrypted Private Information of Class Members will end up for sale to
24 identity thieves on the dark web, if it has not already, or it could simply fall into the hands of
25 companies that will use the detailed Private Information for targeted marketing without the approval
26 of Plaintiff and Class Members. Unauthorized individuals can easily access the Private Information
27 of Plaintiff and Class Members.
28

41. To prevent and detect cyber-attacks or ransomware attacks Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].⁶

⁶ See *Human-operated ransomware attacks: A preventable disaster* (Mar 5, 2020), <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Nov. 15, 2023).

1 42. Given that Defendants were storing patients' Private Information, Defendants could
2 and should have implemented all of the above measures to prevent and detect cyberattacks.

3 43. The Data Breach indicates that Defendants failed to adequately implement one or
4 more of the above measures to prevent cyberattacks, resulting in the Data Breach and, upon
5 information and belief, the exposure of the Private Information of over 3.89 million patients,
6 including that of Plaintiff and Class Members.
7

8 **C. *Defendants Acquire, Collect, And Store Plaintiff's and Class Members' Private***
9 ***Information.***

10 44. Defendants acquire, collect, and store a massive amount of Private Information in the
11 regular course of their business.

12 45. As a condition of obtaining medical services at Defendants, Defendants require that
13 patients, former patients, and other personnel entrust it with highly sensitive personal information.

14 46. By obtaining, collecting, and using Plaintiff's and Class Members' Private
15 Information, Defendants assumed legal and equitable duties and knew or should have known that it
16 was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.
17

18 47. Plaintiff and Class Members have taken reasonable steps to maintain the
19 confidentiality of their Private Information and would not have entrusted it to Defendants absent a
20 promise to safeguard that information.

21 48. Plaintiff and the Class Members relied on Defendants to keep their Private
22 Information confidential and securely maintained, to use this information for business purposes only,
23 and to make only authorized disclosures of this information.
24
25
26
27
28

D. *Defendants Knew or Should Have Known of the Risk Because Healthcare Entities in Possession of Private Information Are Particularly Susceptable to Cyber Attacks.*

49. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting healthcare entities that collect and store Private Information, like Defendants, preceding the date of the breach.

50. Data breaches, including those perpetrated against healthcare entities that store Private Information in their systems, have become widespread.

51. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.⁷

52. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658), compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.⁸

53. Indeed, cyber-attacks, such as the one experienced by Defendants, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals...because they often have lesser IT defenses and a high incentive to regain access to their data quickly."⁹

54. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including American Medical Collection Agency (25 million patients, March

⁷ See 2021 Data Breach Annual Report (ITRC, Jan. 2022), <https://notified.idtheftcenter.org/s/>, at 6.

⁸ *Id.*

⁹ https://www.law360.com/consumerprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0-aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=consumerprotection (last visited Nov. 15, 2023).

1 2019), University of Washington Medicine (974,000 patients, December 2018), Florida Orthopedic
2 Institute (640,000 patients, July 2020), Wolverine Solutions Group (600,000 patients, September
3 2018), Oregon Department of Human Services (645,000 patients, March 2019), Elite Emergency
4 Physicians (550,000 patients, June 2020), Magellan Health (365,000 patients, April 2020), and BJC
5 Health System (286,876 patients, March 2020), Defendants knew or should have known that its
6 electronic records would be targeted by cybercriminals.

7
8 55. Defendants knew and understood that unprotected or exposed Private Information in
9 the custody of healthcare services entities, like Defendants, is valuable and highly sought after by
10 nefarious third parties seeking to illegally monetize that Private Information through unauthorized
11 access.

12
13 56. At all relevant times, Defendants knew, or reasonably should have known, of the
14 importance of safeguarding the Private Information of Plaintiff and Class Members and of the
15 foreseeable consequences that would occur if Defendants' data security system was breached,
16 including, specifically, the significant costs that would be imposed on Plaintiff and Class Members
17 as a result of a breach.

18
19 57. Plaintiff and Class Members now face years of constant surveillance of their financial
20 and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur
21 such damages in addition to any fraudulent use of their Private Information.

22
23 58. The injuries to Plaintiff and Class Members were directly and proximately caused by
24 Defendants' failure to implement or maintain adequate data security measures for the Private
25 Information of Plaintiff and Class Members.

26
27 59. The ramifications of Defendants' failure to keep secure the Private Information of
28 Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—
particularly Social Security numbers and PHI—fraudulent use of that information and damage to
victims may continue for years.

E. Value Of Personally Identifiable Information

60. The Federal Trade Commission (“FTC”) defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁰ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹¹

61. The Private Information of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web.

62. Numerous sources cite dark web pricing for stolen identity credentials.¹² For example, Private Information can be sold at a price ranging from \$40 to \$200.¹³ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹⁴

63. PII can sell for as much as \$363 per record according to the Infosec Institute.¹⁵ PII is particularly valuable because criminals can use it to target victims with frauds and scams.

64. Identity thieves use stolen Private Information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

¹⁰ 17 C.F.R. § 248.201 (2013).

¹¹ *Id.*

¹² *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last visited Nov. 15, 2023).

¹³ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Nov. 15, 2023).

¹⁴ *In the Dark*, VPNOverview, 2019, <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Nov. 15, 2023).

¹⁵ *See Ashiq Ja, Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/> (last visited Nov. 15, 2023).

65. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

66. Theft of PHI is also gravely serious: "[a] thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."

67. According to account monitoring company LogDog, medical data sells for \$50 and up on the Dark Web.¹⁶

68. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

69. Driver's license numbers are also incredibly valuable. "Hackers harvest license numbers because they're a very valuable piece of information. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about \$1200 on the Dark Web. On its own, a forged license can sell for around \$200."¹⁷

70. According to national credit bureau Experian:

¹⁶ Lisa Vaas, *Ransomware Attacks Paralyze, and Sometimes Crush, Hospitals*, Naked Security (Oct. 3, 2019), <https://nakedsecurity.sophos.com/2019/10/03/ransomware-attacks-paralyze-and-sometimes-crush-hospitals/#content> (last visited Nov. 15, 2023).

¹⁷ <https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3e4755c38658> (last visited Nov. 15, 2023).

1 A driver's license is an identity thief's paradise. With that one card, someone knows
 2 your birthdate, address, and even your height, eye color, and signature. If someone
 3 gets your driver's license number, it is also concerning because it's connected to your
 4 vehicle registration and insurance policies, as well as records on file with the
 5 Department of Motor Vehicles, place of employment (that keep a copy of your
 6 driver's license on file), doctor's office, government agencies, and other entities.
 7 Having access to that one number can provide an identity thief with several pieces of
 8 information they want to know about you. Next to your Social Security number, your
 9 driver's license number is one of the most important pieces of information to keep
 10 safe from thieves.

71. According to cybersecurity specialty publication CPO Magazine, "[t]o those
 unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless
 piece of information to lose if it happens in isolation."¹⁸ However, this is not the case. As
 cybersecurity experts point out¹⁹:

It's a gold mine for hackers. With a driver's license number, bad actors can
 manufacture fake IDs, slotting in the number for any form that requires ID
 verification, or use the information to craft curated social engineering phishing
 attacks.

72. Victims of driver's license number theft also often suffer unemployment benefit
 fraud, as described in a recent New York Times article.²⁰

73. The fraudulent activity resulting from the Data Breach may not come to light for
 years. There may be a time lag between when harm occurs versus when it is discovered, and also
 between when Private Information is stolen and when it is used. According to the U.S. Government
 Accountability Office ("GAO"), which conducted a study regarding data breaches²¹:

¹⁸ <https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/> (last visited Nov. 15, 2023).

¹⁹ *Id.*

²⁰ *How Identity Thieves Took My Wife for a Ride*, NY Times, April 27, 2021, available at: <https://www.nytimes.com/2021/04/27/your-money/identity-theft-auto-insurance.html> (last visited Nov. 15, 2023).

²¹ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Nov. 15, 2023).

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

74. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.²² Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.²³ Each of these fraudulent activities is difficult to detect. An individual may not know that his or his Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

75. Moreover, it is not an easy task to change or cancel a stolen Social Security number²⁴:

An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."

76. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card

²² *Identity Theft and Your Social Security number*, Social Security Administration (2018), <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Nov. 15, 2023).

²³ *Id.*

²⁴ Brian Naylor, *Victims of Social Security number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft> (last visited Nov. 15, 2023).

1 information, personally identifiable information and Social Security numbers are worth more than
 2 10x on the black market.”²⁵

3 77. Based on the foregoing, the information compromised in the Data Breach is
 4 significantly more valuable than the loss of, for example, credit card information in a retailer data
 5 breach because, there, victims can cancel or close credit and debit card accounts. The information
 6 compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to
 7 change—names, dates of birth, and PHI.
 8

9 **F. Defendants Fail to Comply with FTC Guidelines.**

10 78. The Federal Trade Commission (“FTC”) has promulgated numerous guides for
 11 businesses which highlight the importance of implementing reasonable data security practices.
 12 According to the FTC, the need for data security should be factored into all business decision-
 13 making.
 14

15 79. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide*
 16 *for Business*, which established cyber-security guidelines for businesses. These guidelines note that
 17 businesses should protect the personal patient information that they keep; properly dispose of
 18 personal information that is no longer needed; encrypt information stored on computer networks;
 19 understand their network’s vulnerabilities; and implement policies to correct any security
 20 problems.²⁶
 21
 22
 23
 24

25 ²⁵ Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card*
 26 *Numbers*, Computer World (Feb. 6, 2015), [http://www.itworld.com/article/2880960/anthem-hack-](http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html)
 27 [personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html](http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html) (last visited Nov. 15,
 28 2023).

²⁶ *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016),
[https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)
[information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf) (last visited Nov. 15, 2023).

1 80. The guidelines also recommend that businesses use an intrusion detection system to
2 expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is
3 attempting to hack the system; watch for large amounts of data being transmitted from the system;
4 and have a response plan ready in the event of a breach.²⁷

5
6 81. The FTC further recommends that companies not maintain Private Information
7 longer than is needed for authorization of a transaction; limit access to sensitive data; require
8 complex passwords to be used on networks; use industry-tested methods for security; monitor for
9 suspicious activity on the network; and verify that third-party service providers have implemented
10 reasonable security measures.

11 82. The FTC has brought enforcement actions against healthcare entities for failing to
12 protect patient data adequately and reasonably, treating the failure to employ reasonable and
13 appropriate measures to protect against unauthorized access to confidential consumer data as an
14 unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTCA”),
15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take
16 to meet their data security obligations.

17
18 83. These FTC enforcement actions include actions against healthcare providers like
19 Defendants. *See, e.g., In the Matter of LabMd, Inc., A Corp*, 2016-2 Trade Cas. (Defendants) ¶
20 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) (“[T]he Commission concludes that
21 LabMD’s data security practices were unreasonable and constitute an unfair act or practice in
22 violation of Section 5 of the FTC Act.”).

23
24 84. Defendants failed to properly implement basic data security practices.

25
26
27
28 ²⁷ *Id.*

85. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

86. Upon information and belief, Defendants were at all times fully aware of their obligation to protect the Private Information of its patients. Defendants were also aware of the significant repercussions that would result from its failure to do so.

G. *Defendants Fail to Comply with HIPAA Guidelines.*

87. Northwell is a covered Business Associate under HIPAA (45 C.F.R. § 160.103) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

88. Both Defendants are subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").²⁸ See 42 U.S.C. § 17921, 45 C.F.R. § 160.103.

89. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

90. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

²⁸ HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

1 91. HIPAA requires “compl[iance] with the applicable standards, implementation
2 specifications, and requirements” of HIPAA “with respect to electronic protected health
3 information.” 45 C.F.R. § 164.302.

4 92. “Electronic protected health information” is “individually identifiable health
5 information . . . that is (i) transmitted by electronic media; maintained in electronic media.” 45 C.F.R.
6 § 160.103.

7 93. HIPAA’s Security Rule requires Defendants to do the following:

8 a. Ensure the confidentiality, integrity, and availability of all electronic protected
9 health information the covered entity or business associate creates, receives, maintains, or
10 transmits;

11 b. Protect against any reasonably anticipated threats or hazards to the security or
12 integrity of such information;

13 c. Protect against any reasonably anticipated uses or disclosures of such
14 information that are not permitted; and

15 d. Ensure compliance by its workforce.

16 94. HIPAA also requires Defendants to “review and modify the security measures
17 implemented . . . as needed to continue provision of reasonable and appropriate protection of
18 electronic protected health information.” 45 C.F.R. § 164.306(e). Additionally, Defendants is
19 required under HIPAA to “[i]mplement technical policies and procedures for electronic information
20 systems that maintain electronic protected health information to allow access only to those persons
21 or software programs that have been granted access rights.” 45 C.F.R. § 164.312(a)(1).

22 95. HIPAA and HITECH also obligated Defendants to implement policies and
23 procedures to prevent, detect, contain, and correct security violations, and to protect against uses or
24 disclosures of electronic protected health information that are reasonably anticipated but not
25
26
27
28

permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. § 17902.

96. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendants to provide notice of the Data Breach to each affected individual “without unreasonable delay and *in no case later than 60 days following discovery of the breach.*”²⁹

97. HIPAA requires a covered entity to have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

98. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

99. HIPAA also requires the Office of Civil Rights (“OCR”), within the Department of Health and Human Services (“HHS”), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, “HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements of the Security Rule.” US Department of Health & Human Services, Security Rule Guidance Material.³⁰ The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says “represent the industry standard for good

²⁹ Breach Notification Rule, U.S. DEP’T OF HEALTH & HUMAN SERVS., <https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html> (emphasis added) (last visited Nov. 15, 2023).

³⁰ <http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html> (last visited Nov. 15, 2023).

1 business practices with respect to standards for securing e-PHI.” US Department of Health & Human
2 Services, Guidance on Risk Analysis.³¹

3 **H. *Defendants Fail to Comply with Industry Standards.***

4 100. As noted above, experts studying cyber security routinely identify entities in
5 possession of Private Information as being particularly vulnerable to cyberattacks because of the
6 value of the Private Information which they collect and maintain.

7 101. Several best practices have been identified that, at a minimum, should be
8 implemented by healthcare entities in possession of Private Information, like Defendants, including
9 but not limited to: educating all employees; strong passwords; multi-layer security, including
10 firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key;
11 multi-factor authentication; backup data and limiting which employees can access sensitive data.
12 Defendants failed to follow these industry best practices, including a failure to implement multi-
13 factor authentication.

14 102. Other best cybersecurity practices that are standard in the healthcare industry include
15 installing appropriate malware detection software; monitoring and limiting the network ports;
16 protecting web browsers and email management systems; setting up network systems such as
17 firewalls, switches and routers; monitoring and protection of physical security systems; protection
18 against any possible communication system; training staff regarding critical points. Defendants
19 failed to follow these cybersecurity best practices, including failure to train staff.

20 103. Defendants failed to meet the minimum standards of any of the following
21 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-
22 1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1,

23
24
25
26
27
28 ³¹ <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last
visited Nov. 15, 2023).

PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

104. These foregoing frameworks are existing and applicable industry standards in the healthcare industry, and upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

I. Common Injuries & Damages

105. As a result of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of Private Information ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); (d) diminution of value of their Private Information; (e) invasion of privacy; and (f) the continued risk to their Private Information, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Private Information.

J. The Data Breach Increases Victims' Risk of Identity Theft.

106. Plaintiff and Class Members are at a heightened risk of identity theft for years to come.

107. The unencrypted Private Information of Class Members will end up for sale on the dark web because that is the *modus operandi* of hackers. In addition, unencrypted Private Information may fall into the hands of companies that will use the detailed Private Information for

1 targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals
2 can easily access the Private Information of Plaintiff and Class Members.

3 108. The link between a data breach and the risk of identity theft is simple and well
4 established. Criminals acquire and steal Private Information to monetize the information. Criminals
5 monetize the data by selling the stolen information on the black market to other criminals who then
6 utilize the information to commit a variety of identity theft related crimes discussed below.

7 109. Because a person's identity is akin to a puzzle with multiple data points, the more
8 accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on
9 the victim's identity—or track the victim to attempt other hacking crimes against the individual to
10 obtain more data to perfect a crime.

11 110. For example, armed with just a name and date of birth, a data thief can utilize a
12 hacking technique referred to as “social engineering” to obtain even more information about a
13 victim's identity, such as a person's login credentials or Social Security number. Social engineering
14 is a form of hacking whereby a data thief uses previously acquired information to manipulate and
15 trick individuals into disclosing additional confidential or personal information through means such
16 as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point
17 for these additional targeted attacks on the victim.

18 111. One such example of criminals piecing together bits and pieces of compromised
19 Private Information for profit is the development of “Fullz” packages.³²

20
21
22
23
24 ³² “Fullz” is fraudster speak for data that includes the information of the victim, including, but not
25 limited to, the name, address, credit card information, social security number, date of birth, and more.
26 As a rule of thumb, the more information you have on a victim, the more money that can be made
27 off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding
28

112. With “Fullz” packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

113. The development of “Fullz” packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiff’ and Class Members’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

114. The existence and prevalence of “Fullz” packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiff and the other Class Members.

up to \$100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even “dead Fullz,” which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a “mule account” (an account that will accept a fraudulent money transfer from a compromised account) without the victim’s knowledge. *See, e.g.,* Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), <https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-> (last visited Nov. 15, 2023).

1 115. Thus, even if certain information (such as telephone numbers) was not stolen in the
2 data breach, criminals can still easily create a comprehensive “Fullz” package.

3 116. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to
4 crooked operators and other criminals (like illegal and scam telemarketers).
5

6 **K. *Loss of Time to Mitigate Risk of Identity Theft and Fraud***

7 117. As a result of the recognized risk of identity theft, when a Data Breach occurs, and
8 an individual is notified by a company that their Private Information was compromised, as in this
9 Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous
10 situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity
11 theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose
12 the individual to greater financial harm—yet, the resource and asset of time has been lost.
13

14 118. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class
15 Members must, as Defendants’ Notice Letter encourages, monitor their financial accounts for many
16 years to mitigate the risk of identity theft.

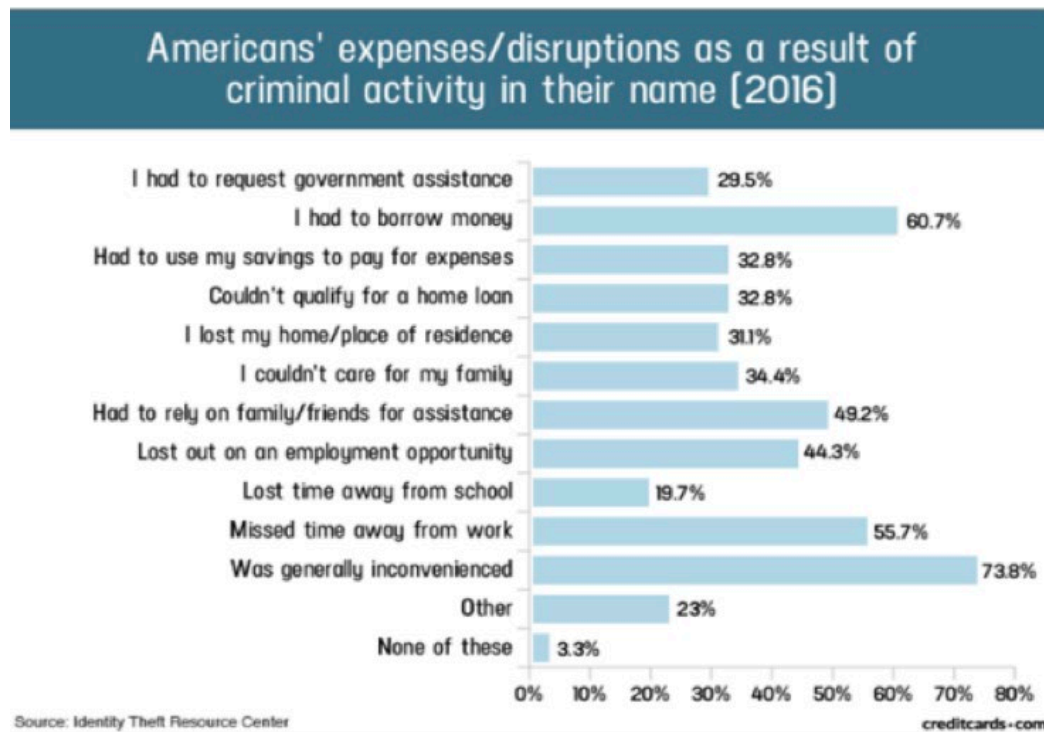
17 119. Plaintiff and Class Members have spent, and will spend additional time in the future,
18 on a variety of prudent actions, such as contacting their banks to ensure their financial accounts are
19 secured.
20

21 120. Plaintiff’s mitigation efforts are consistent with the U.S. Government Accountability
22 Office that released a report in 2007 regarding data breaches (“GAO Report”) in which it noted that
23 victims of identity theft will face “substantial costs and time to repair the damage to their good name
24 and credit record.”³³
25
26

27 ³³ See U.S. Government Accountability Office, GAO-07-737, *Personal Information: Data Breaches*
28 *Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), <https://www.gao.gov/new.items/d07737.pdf>.

121. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.³⁴

122. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:³⁵



123. And for those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches

³⁴ See Federal Trade Commission, *Identity Theft.gov*, <https://www.identitytheft.gov/Steps> (last visited Nov. 15, 2023).

³⁵ Jason Steele, *Credit Card and ID Theft Statistics*, 10/24/2017, <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php> (last visited Nov. 15, 2023).

1 (“GAO Report”) in which it noted that victims of identity theft will face “substantial costs and time
2 to repair the damage to their good name and credit record.”³⁶

3 **L. Diminution Value of Private Information**

4 124. PII and PHI are valuable property rights.³⁷ Their value is axiomatic, considering the
5 value of Big Data in corporate America and the consequences of cyber thefts include heavy prison
6 sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information
7 has considerable market value.
8

9 125. An active and robust legitimate marketplace for Private Information exists. In 2019,
10 the data brokering industry was worth roughly \$200 billion.³⁸

11 126. In fact, the data marketplace is so sophisticated that consumers can actually sell their
12 non-public information directly to a data broker who in turn aggregates the information and provides
13 it to marketers or app developers.³⁹
14

15 127. Consumers who agree to provide their web browsing history to the Nielsen
16 Corporation can receive up to \$50.00 a year.⁴⁰
17
18
19

20
21 ³⁶ See “Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However,
22 the Full Extent Is Unknown,” at 2, U.S. Government Accountability Office, June 2007,
<https://www.gao.gov/new.items/d07737.pdf> (last visited Nov. 15, 2023) (“GAO Report”).

23 ³⁷ See, e.g., Randall T. Soma, et al, Corporate Privacy Trend: The “Value” of Personally Identifiable
24 Information (“Private Information”) Equals the “Value” of Financial Assets, 15 Rich. J.L. & Tech.
25 11, at *3-4 (2009) (“Private Information, which companies obtain at little cost, has quantifiable value
that is rapidly reaching a level comparable to the value of traditional financial assets.”) (citations
omitted).

26 ³⁸ <https://www.latimes.com/business/story/2019-11-05/column-data-brokers> (last visited Nov. 15,
2023).

27 ³⁹ <https://datacoup.com/> (last visited Nov. 15, 2023).

28 ⁴⁰ Nielsen Computer & Mobile Panel, Frequently Asked Questions,
<https://computermobilepanel.nielsen.com/ui/US/en/faqen.html> (last visited Nov. 15, 2023).

1 128. Conversely sensitive PII can sell for as much as \$363 per record on the dark web
2 according to the Infosec Institute.⁴¹

3 129. As a result of the Data Breach, Plaintiff's and Class Members' Private Information,
4 which has an inherent market value in both legitimate and dark markets, has been damaged and
5 diminished by its compromise and unauthorized release. However, this transfer of value occurred
6 without any consideration paid to Plaintiff or Class Members for their property, resulting in an
7 economic loss. Moreover, Private Information is now readily available, and the rarity of the Data
8 has been lost, thereby causing additional loss of value.

9 130. Based on the foregoing, the information compromised in the Data Breach is
10 significantly more valuable than the loss of, for example, credit card information in a retailer data
11 breach because, there, victims can cancel or close credit and debit card accounts. The information
12 compromised in this Data Breach is static and impossible to "close" and difficult, if not impossible,
13 to change, e.g., names, Social Security numbers, dates of birth, and PHI.

14 131. Among other forms of fraud, identity thieves may obtain driver's licenses,
15 government benefits, medical services, and housing or even give false information to police.

16 132. The fraudulent activity resulting from the Data Breach may not come to light for
17 years.

18 133. At all relevant times, Defendants knew, or reasonably should have known, of the
19 importance of safeguarding the Private Information of Plaintiff and Class Members, and of the
20 foreseeable consequences that would occur if Defendants' data security system was breached,
21
22
23
24
25
26

27 ⁴¹ See Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015),
28 <https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/>
(last visited Nov. 15, 2023).

1 including, specifically, the significant costs that would be imposed on Plaintiff and Class Members
2 as a result of a breach.

3 134. Defendants was, or should have been, fully aware of the unique type and the
4 significant volume of data on Defendants' network, amounting to over three hundred thousand
5 individuals' detailed personal information, upon information and belief, and thus, the significant
6 number of individuals who would be harmed by the exposure of the unencrypted data.
7

8 135. The injuries to Plaintiff and Class Members were directly and proximately caused by
9 Defendants' failure to implement or maintain adequate data security measures for the Private
10 Information of Plaintiff and Class Members.

11 **L. *Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary.***

12 136. Given the type of targeted attack in this case and sophisticated criminal activity, the
13 type of Private Information involved, the volume of data obtained in the Data Breach, and Plaintiff's
14 Private Information already being disseminated on the dark web, there is a strong probability that
15 entire batches of stolen information have been placed, or will be placed, on the black market/dark
16 web for sale and purchase by criminals intending to utilize the Private Information for identity theft
17 crimes—*e.g.*, opening bank accounts in the victims' names to make purchases or to launder money;
18 filing false tax returns; taking out loans or lines of credit; or filing false unemployment claims.
19

20 137. Such fraud may go undetected until debt collection calls commence months, or even
21 years, later. An individual may not know that his or his Social Security number was used to file for
22 unemployment benefits until law enforcement notifies the individual's employer of the suspected
23 fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return
24 is rejected.
25

26 138. Furthermore, the information accessed and disseminated in the Data Breach is
27 significantly more valuable than the loss of, for example, credit card information in a retailer data
28

breach, where victims can easily cancel or close credit and debit card accounts.⁴² The information disclosed in this Data Breach is impossible to “close” and difficult, if not impossible, to change (such as Social Security numbers).

139. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

140. The retail cost of credit monitoring and identity theft monitoring can cost around \$200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants’ Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendants’ failure to safeguard their Private Information.

M. Plaintiff’s Experience

141. Plaintiff Neil Levitt is a patient of Northwell and has seen a physician there as recently as May of 2023. He is also a former employee, having worked there over ten years ago.

142. In order to obtain healthcare services from Defendants, he was required to provide his Private Information, indirectly or directly, to Defendants.

143. At the time of the Data Breach—between around March 27, 2023 and May 2, 2023—Defendants retained Plaintiff’s Private Information in their systems, and still has his Private Information currently.

144. Plaintiff is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other

⁴² See Jesse Damiani, *Your Social Security Number Costs \$4 On The Dark Web, New Report Finds*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/jessedamiani/2020/03/25/your-social-security-number-costs-4-on-the-dark-web-new-report-finds/?sh=6a44b6d513f1>.

1 unsecured source. Plaintiff would not have entrusted his Private Information to Defendants had he
2 known of Defendants' lax data security policies.

3 145. Plaintiff received the Notice Letter, by U.S. mail, directly from Defendants, dated
4 November 3, 2023. *See* Ex. A. According to the Notice Letter, Plaintiff's PII and PHI was
5 improperly accessed and obtained by unauthorized third parties. *Id.*

6 146. As a result of the Data Breach, and at the direction of Defendants' Notice Letter,
7 Plaintiff made and continues to make reasonable efforts to mitigate the impact of the Data Breach.
8 Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise
9 would have spent on other activities, including but not limited to work and/or recreation. This time
10 has been lost forever and cannot be recaptured.

11 147. Plaintiff diligently monitors his identity and credit through accounts he reviews and
12 pays for. He regularly receives notices from companies, including Credit Karma and Kroll, that
13 monitor his identity and credit. Recently, he has been notified of suspicious activity, including a
14 notice that his Private Information may be available on the dark web. Plaintiff reasonably believes
15 this suspicious activity is as a result of the Data Breach.

16 148. Plaintiff suffered actual injury from having his Private Information compromised as
17 a result of the Data Breach including, but not limited to: (i) his Private Information being
18 disseminated on the dark web; (ii) an increase in spam calls, texts, and/or emails; (iii) lost or
19 diminished value of his Private Information; (iv) lost opportunity costs associated with attempting
20 to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (v)
21 invasion of privacy; (vi) loss of benefit of the bargain; and (vii) the continued and certainly increased
22 risk to his Private Information, which: (a) remains unencrypted and available for unauthorized third
23 parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to
24 further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate
25 measures to protect the Private Information.

1 149. The Data Breach has caused Plaintiff to suffer fear, anxiety, and stress, which has
2 been compounded by the fact that Defendants have still not fully informed him of key details about
3 the Data Breach.

4 150. As a result of the Data Breach, Plaintiff anticipates spending considerable time and
5 money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

6 151. As a result of the Data Breach, Plaintiff is at a present risk and will continue to be at
7 increased risk of identity theft and fraud for years to come.

8 152. Plaintiff has a continuing interest in ensuring that his Private Information, which,
9 upon information and belief, remains backed up in Defendants' possession, is protected and
10 safeguarded from future breaches.

11
12 V. CLASS ACTION ALLEGATIONS

13
14 153. Plaintiff brings this action individually and on behalf of all other persons similarly
15 situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(2), and 23(b)(3).

16 154. Specifically, Plaintiff proposes the following class definitions, subject to amendment
17 as appropriate:

18 All individuals who reside in the United States whose Private
19 Information was exposed in the Data Breach involving Defendants
20 (the "Class").

21 155. Excluded from the Classes are Defendants and their parents or subsidiaries, any
22 entities in which they have a controlling interest, as well as their officers, directors, affiliates, legal
23 representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom
24 this case is assigned as well as their judicial staff and immediate family members.

25 156. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes,
26 as well as add subclasses, before the Court determines whether certification is appropriate.

27 157. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a),
28 (b)(2), and (b)(3).

1 158. Numerosity: The members of the Classes are so numerous that joinder of all members
2 is impracticable, if not completely impossible. Upon information and belief, there are in excess of 3
3 million individuals whose Private Information may have been improperly accessed in the Data
4 Breach. The Class is apparently identifiable within Defendants' records, and Defendants have
5 already identified these individuals (as evidenced by sending them breach notification letters).
6

7 159. Commonality. There are questions of law and fact common to the Classes which
8 predominate over any questions affecting only individual Class Members. These common questions
9 of law and fact include, without limitation:

- 10 a. Whether Defendants engaged in the conduct alleged herein;
- 11 b. When Defendants learned of the Data Breach;
- 12 c. Whether Defendants' response to the Data Breach was adequate;
- 13 d. Whether Defendants unlawfully lost or disclosed Plaintiff's and Class
14 Members' Private Information;
- 15 e. Whether Defendants failed to implement and maintain reasonable security
16 procedures and practices appropriate to the nature and scope of the Private Information
17 compromised in the Data Breach;
- 18 f. Whether Defendants owed a duty to Class Members to safeguard their Private
19 Information;
- 20 g. Whether Defendants breached their duties to Class Members to safeguard
21 their Private Information;
- 22 h. Whether hackers obtained Class Members' Private Information via the Data
23 Breach;
- 24 i. Whether Defendants had a legal duty to provide timely and accurate notice of
25 the Data Breach to Plaintiff and the Class Members;
- 26
27
28

j. Whether Defendants breached their duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

k. Whether Defendants knew or should have known that Defendants' data security systems and monitoring processes as such relate to its secure file transfer services were deficient;

l. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

m. Whether Defendants' conduct was negligent;

n. Whether Defendants were unjustly enriched;

o. Whether Plaintiff and Class Members are entitled to actual and/or statutory damages;

p. Whether Plaintiff and Class Members are entitled to credit or identity monitoring and monetary relief; and

q. Whether Plaintiff and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

160. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class Member, was compromised in the Data Breach.

161. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

162. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over

any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

163. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

164. Class certification is also appropriate. Defendants have acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate to the Class as a whole.

165. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to the names and addresses and/or email addresses of Class Members affected by the Data Breach.

VI. CLAIMS FOR RELIEF

COUNT I

Negligence

(On Behalf of Plaintiff and the Class)

166. Plaintiff restates and realleges facts set forth above as if fully alleged herein.

167. Defendants collect the Private Information of its patients, including that of Plaintiff and Class Members, in the ordinary course of providing their healthcare and medical transcription services.

1 168. Plaintiff and Class Members entrusted Defendants with their Private Information,
2 directly or indirectly, with the understanding that Defendants would safeguard their information.

3 169. Defendants had full knowledge of the sensitivity of the Private Information and the
4 types of harm that Plaintiff and Class Members could and would suffer if the Private Information
5 were wrongfully disclosed.
6

7 170. By assuming the responsibility to collect and store this data, and in fact doing so, and
8 sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means
9 to secure and safeguard their computer property—and Class Members' Private Information held
10 within it—to prevent disclosure of the information, and to safeguard the information from theft.
11 Defendants' duty included a responsibility to implement processes by which they could detect a
12 breach of its security systems in a reasonably expeditious period of time and to give prompt notice
13 to those affected in the case of a data breach.
14

15 171. Defendants had a duty to employ reasonable security measures under Section 5 of the
16 Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits “unfair . . . practices in or affecting
17 commerce,” including, as interpreted and enforced by the FTC, the unfair practice of failing to use
18 reasonable measures to protect confidential data.
19

20 172. Defendants' duty to use reasonable security measures under HIPAA required
21 Defendants to “reasonably protect” confidential data from “any intentional or unintentional use or
22 disclosure” and to “have in place appropriate administrative, technical, and physical safeguards to
23 protect the privacy of protected health information.” 45 C.F.R. § 164.530(c)(1). Some or all of the
24 healthcare and/or medical information at issue in this case constitutes “protected health information”
25 within the meaning of HIPAA.
26

27 173. Defendants owed a duty of care to Plaintiff and Class Members to provide data
28 security consistent with industry standards and other requirements discussed herein, and to ensure

1 that its systems and networks, and the personnel responsible for them, adequately protected the
2 Private Information.

3 174. Defendants' duty of care to use reasonable security measures arose as a result of the
4 special relationship that existed between Defendants and Plaintiff and Class Members. That special
5 relationship arose because Plaintiff and the Class entrusted Defendants with their confidential
6 Private Information, a necessary part of being patients at Defendants.

7 175. Defendants' duty to use reasonable care in protecting confidential data arose not only
8 as a result of the statutes and regulations described above, but also because Defendants are bound
9 by industry standards to protect confidential Private Information.
10

11 176. Defendants were subject to an "independent duty," untethered to any contract
12 between Defendants and Plaintiff or the Class.

13 177. Defendants also had a duty to exercise appropriate clearinghouse practices to remove
14 former patients' Private Information it was no longer required to retain pursuant to regulations.

15 178. Moreover, Defendants had a duty to promptly and adequately notify Plaintiff and the
16 Class of the Data Breach.

17 179. Defendants had and continue to have a duty to adequately disclose that the Private
18 Information of Plaintiff and the Class within Defendants' possession might have been compromised,
19 how it was compromised, and precisely the types of data that were compromised and when. Such
20 notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair
21 any identity theft and the fraudulent use of their Private Information by third parties.

22 180. Defendants breached their duties, pursuant to the FTC Act, HIPAA, and other
23 applicable standards, and thus were negligent, by failing to use reasonable measures to protect Class
24 Members' Private Information. The specific negligent acts and omissions committed by Defendants
25 include, but are not limited to, the following:
26
27
28

- a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;
- b. Failing to adequately monitor the security of their networks and systems;
- c. Failure to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;
- d. Allowing unauthorized access to Class Members' Private Information;
- e. Failing to detect in a timely manner that Class Members' Private Information had been compromised;
- f. Failing to remove former patients' Private Information it was no longer required to retain pursuant to regulations,
- g. Failing to timely and adequately notify Class Members about the Data Breach and its scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and
- h. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

181. Defendants violated Section 5 of the FTC Act and HIPAA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

182. Plaintiff and the Class are within the class of persons that the FTC Act and HIPAA were intended to protect.

183. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act and HIPAA were intended to guard against.

184. Defendants' violation of Section 5 of the FTC Act and HIPAA constitutes negligence.

1 185. The FTC has pursued enforcement actions against businesses, which, as a result of
2 their failure to employ reasonable data security measures and avoid unfair and deceptive practices,
3 caused the same harm as that suffered by Plaintiff and the Class.

4 186. A breach of security, unauthorized access, and resulting injury to Plaintiff and the
5 Class was reasonably foreseeable, particularly in light of Defendants' inadequate security practices.

6 187. It was foreseeable that Defendants' failure to use reasonable measures to protect Class
7 Members' Private Information would result in injury to Class Members. Further, the breach of
8 security was reasonably foreseeable given the known high frequency of cyberattacks and data
9 breaches in the healthcare industry.

10 188. Defendants have full knowledge of the sensitivity of the Private Information and the
11 types of harm that Plaintiff and the Class could and would suffer if the Private Information were
12 wrongfully disclosed.

13 189. Plaintiff and the Class were the foreseeable and probable victims of any inadequate
14 security practices and procedures. Defendants knew or should have known of the inherent risks in
15 collecting and storing the Private Information of Plaintiff and the Class, the critical importance of
16 providing adequate security of that Private Information, and the necessity for encrypting Private
17 Information stored on Defendants' systems.

18 190. It was therefore foreseeable that the failure to adequately safeguard Class Members'
19 Private Information would result in one or more types of injuries to Class Members.

20 191. Plaintiff and the Class had no ability to protect their Private Information that was in,
21 and remains in, Defendants' possession.

22 192. Defendants were in an exclusive position to protect against the harm suffered by
23 Plaintiff and the Class as a result of the Data Breach.

24 193. Defendants' duty extended to protecting Plaintiff and the Class from the risk of
25 foreseeable criminal conduct of third parties, which has been recognized in situations where the
26

1 actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to
2 guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second)
3 of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific
4 duty to reasonably safeguard personal information.

5
6 194. Defendants have admitted that the Private Information of Plaintiff and the Class was
7 wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

8 195. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the
9 Class, the Private Information of Plaintiff and the Class would not have been compromised.

10 196. There is a close causal connection between Defendants' failure to implement security
11 measures to protect the Private Information of Plaintiff and the Class and the harm, or risk of
12 imminent harm, suffered by Plaintiff and the Class. The Private Information of Plaintiff and the Class
13 was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in
14 safeguarding such Private Information by adopting, implementing, and maintaining appropriate
15 security measures.

16
17 197. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class
18 have suffered and will suffer injury, including but not limited to: (i) Plaintiff's Private Information
19 being disseminated on the dark web; (ii) Plaintiff experiencing an increase in spam calls, texts, and/or
20 emails; (iii) lost or diminished value of their Private Information; (iv) lost opportunity costs
21 associated with attempting to mitigate the actual consequences of the Data Breach, including but not
22 limited to lost time; (v) invasion of privacy; (vi) loss of benefit of the bargain; and (vii) the continued
23 and certainly increased risk to their Private Information, which: (a) remains unencrypted and
24 available for unauthorized third parties to access and abuse; and (b) remains backed up in
25 Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails
26 to undertake appropriate and adequate measures to protect the Private Information.
27
28

198. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

199. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

200. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

201. Defendants' negligent conduct is ongoing, in that it still holds the Private Information of Plaintiff and Class Members in an unsafe and insecure manner.

202. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

203. Plaintiff restates and realleges facts set forth above if fully set forth herein.

204. Plaintiff and Class Members were required to provide their Private Information to Defendants as a condition of receiving healthcare services from Defendants.

205. Plaintiff and the Class entrusted their Private Information to Defendants. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and

1 compromised or stolen.

2 206. In entering into such implied contracts, Plaintiff and Class Members reasonably
3 believed and expected that Defendants' data security practices complied with relevant laws and
4 regulations and were consistent with industry standards.

5 207. Implicit in the agreement between Plaintiff and Class Members and the Defendants
6 to provide Private Information, was the latter's obligation to: (a) use such Private Information for
7 business purposes only, (b) take reasonable steps to safeguard that Private Information, (c) prevent
8 unauthorized disclosures of the Private Information, (d) provide Plaintiff and Class Members with
9 prompt and sufficient notice of any and all unauthorized access and/or theft of their Private
10 Information, (e) reasonably safeguard and protect the Private Information of Plaintiff and Class
11 Members from unauthorized disclosure or uses, (f) retain the Private Information only under
12 conditions that kept such information secure and confidential.

13 208. The mutual understanding and intent of Plaintiff and Class Members on the one
14 hand, and Defendants, on the other, is demonstrated by their conduct and course of dealing.

15 209. Defendants solicited, offered, and invited Plaintiff and Class Members to provide
16 their Private Information as part of Defendants' regular business practices. Plaintiff and Class
17 Members accepted Defendants' offers and provided their Private Information to Defendants.

18 210. In accepting the Private Information of Plaintiff and Class Members, Defendants
19 understood and agreed that they were required to reasonably safeguard the Private Information
20 from unauthorized access or disclosure.

21 211. On information and belief, at all relevant times Defendants promulgated, adopted,
22 and implemented written privacy policies whereby it expressly promised Plaintiff and Class
23 Members that it would only disclose Private Information under certain circumstances, none of
24 which relate to the Data Breach.

25 212. On information and belief, Defendants further promised to comply with industry
26
27
28

1 standards and to make sure that Plaintiff's and Class Members' Private Information would remain
2 protected.

3 213. Plaintiff and Class Members paid money and provided their Private Information to
4 Defendants with the reasonable belief and expectation that Defendants would use part of its
5 earnings to obtain adequate data security. Defendants failed to do so.
6

7 214. Plaintiff and Class Members would not have entrusted their Private Information to
8 Defendants in the absence of the implied contract between them and Defendants to keep their
9 information reasonably secure.

10 215. Plaintiff and Class Members would not have entrusted their Private Information to
11 Defendants in the absence of their implied promise to monitor their computer systems and networks
12 to ensure that it adopted reasonable data security measures.
13

14 216. Plaintiff and Class Members fully and adequately performed their obligations
15 under the implied contracts with Defendants.

16 217. Defendants breached the implied contracts it made with Plaintiff and the Class by
17 failing to safeguard and protect their personal information, by failing to delete the information of
18 Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them
19 that personal information was compromised as a result of the Data Breach.
20

21 218. As a direct and proximate result of Defendants' breach of the implied contracts,
22 Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit
23 of the bargain.

24 219. Plaintiff and Class Members are entitled to compensatory, consequential, and
25 nominal damages suffered as a result of the Data Breach.

26 220. Plaintiff and Class Members are also entitled to injunctive relief requiring
27 Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit
28 to future annual audits of those systems and monitoring procedures; and (iii) immediately provide

adequate credit monitoring to all Class Members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

221. Plaintiff restates and realleges facts set forth above as if fully alleged herein.

222. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, they paid for services from Defendants and in so doing also provided Defendants with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendants the services that were the subject of the transaction and should have had their Private Information protected with adequate data security.

223. Defendants knew that Plaintiff and Class Members conferred a benefit upon it and has accepted and retained that benefit by accepting and retaining the Private Information entrusted to it. Defendants profited from Plaintiff's retained data and used Plaintiff's and Class Members' Private Information for business purposes.

224. Defendants failed to secure Plaintiff's and Class Members' Private Information and, therefore, did not fully compensate Plaintiff or Class Members for the value that their Private Information provided.

225. Defendants acquired Private Information through inequitable record retention as it failed to disclose the inadequate data security practices previously alleged.

226. If Plaintiff and Class Members had known that Defendants would not use adequate data security practices, procedures, and protocols to adequately monitor, supervise, and secure their Private Information, they would have entrusted their Private Information with Defendants or obtained services from Defendants.

227. Plaintiff and Class Members have no adequate remedy at law.

228. Under the circumstances, it would be unjust for Defendants to be permitted to retain any of the benefits that Plaintiff and Class Members conferred upon it.

1 229. Plaintiff and Class Members are entitled to restitution, and/or damages from
2 Defendants and/or an order proportionally disgorging all profits, benefits, and other compensation
3 obtained by Defendants from its wrongful conduct. This can be accomplished by establishing a
4 constructive trust from which the Plaintiff and Class Members may seek restitution or compensation.
5

6 230. Plaintiff and Class Members may not have an adequate remedy at law against
7 Defendants, and accordingly, they plead this claim for unjust enrichment in addition to, or in the
8 alternative to, other claims pleaded herein.

9 **VII. PRAYER FOR RELIEF**

10 WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment
11 against Defendants and that the Court grants the following:

12 1. For an order certifying the Class, as defined herein, and appointing Plaintiff and his
13 Counsel to represent the Class;
14

15 2. For equitable relief enjoining Defendants from engaging in the wrongful conduct
16 complained of herein pertaining to the misuse and/or disclosure of the Private Information of
17 Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures
18 to Plaintiff and Class Members;
19

20 3. For injunctive relief requested by Plaintiff, including but not limited to, injunctive
21 and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members,
22 including but not limited to an order:

23 i. prohibiting Defendants from engaging in the wrongful and unlawful acts
24 described herein;

25 ii. requiring Defendants to protect, including through encryption, all data
26 collected through the course of their business in accordance with all applicable regulations,
27 industry standards, and federal, state, or local laws.
28

1 iii. requiring Defendants to delete, destroy, and purge the personal identifying
2 information of Plaintiff and Class Members unless Defendants can provide to the Court
3 reasonable justification for the retention and use of such information when weighed against
4 the privacy interests of Plaintiff and Class Members;

5 iv. requiring Defendants to implement and maintain a comprehensive
6 Information Security Program designed to protect the confidentiality and integrity of the PII
7 of Plaintiff and Class Members;

8 v. prohibiting Defendants from maintaining the Private Information of Plaintiff
9 and Class Members on a cloud-based database;

10 vi. requiring Defendants to engage independent third-party security
11 auditors/penetration testers as well as internal security personnel to conduct testing, including
12 simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis,
13 and ordering Defendants to promptly correct any problems or issues detected by such third-
14 party security auditors;

15 vii. requiring Defendants to engage independent third-party security auditors and
16 internal personnel to run automated security monitoring;

17 viii. requiring Defendants to audit, test, and train its security personnel regarding
18 any new or modified procedures;

19 ix. requiring Defendants to segment data by, among other things, creating
20 firewalls and access controls so that if one area of Defendants' network is compromised,
21 hackers cannot gain access to other portions of Defendants' systems;

22 x. requiring Defendants to conduct regular database scanning and securing
23 checks;

24 xi. requiring Defendants to establish an information security training program
25 that includes at least annual information security training for all employees, with additional
26
27
28

1 training to be provided as appropriate based upon the employees' respective responsibilities
2 with handling personal identifying information, as well as protecting the personal identifying
3 information of Plaintiff and Class Members;

4 xii. requiring Defendants to conduct internal training and education routinely and
5 continually, and on an annual basis to inform internal security personnel how to identify and
6 contain a breach when it occurs and what to do in response to a breach;

7
8 xiii. requiring Defendants to implement a system of tests to assess its employees'
9 knowledge of the education programs discussed in the preceding subparagraphs, as well as
10 randomly and periodically testing employees' compliance with Defendants' policies,
11 programs, and systems for protecting personal identifying information;

12
13 xiv. requiring Defendants to implement, maintain, regularly review, and revise as
14 necessary a threat management program designed to appropriately monitor Defendants'
15 information networks for threats, both internal and external, and assess whether monitoring
16 tools are appropriately configured, tested, and updated;

17
18 xv. requiring Defendants to meaningfully educate all Class Members about the
19 threats that they face as a result of the loss of their confidential Private Information to third
20 parties, as well as the steps affected individuals must take to protect themselves;

21
22 xvi. requiring Defendants to implement logging and monitoring programs
23 sufficient to track traffic to and from Defendants' servers; and

24
25 xvii. for a period of 10 years, appointing a qualified and independent third-party
26 assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants'
27 compliance with the terms of the Court's final judgment, to provide such report to the Court
28 and to counsel for the class, and to report any deficiencies with compliance of the Court's
final judgment;

4. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;
5. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
6. For prejudgment interest on all amounts awarded; and
7. Such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of the Class, hereby demands a trial by jury on all issues so triable.

DATED: November 16, 2023

Respectfully submitted,

/s/ Nathan R. Ring

Nathan R. Ring

Nevada State Bar No. 12078

STRANCH, JENNINGS & GARVEY, LLC

2100 W. Charleston Boulevard, Suite 208

Las Vegas, NV 89102

Jeff Ostrow (*pro hac vice* forthcoming)

Ken Grunfeld (*pro hac vice* forthcoming)

KOPELOWITZ OSTROW P.A.

One West Las Olas Blvd., Suite 500

Fort Lauderdale, Florida 33301

Telephone: 954-525-4100

ostrow@kolawyers.com

grunfeld@kolawyers.com

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

November 3, 2023

K0005-L2 -1621531 T05021 P095 *****SCH 5-DIGIT 11520

NEIL H LEVITT



Re: **NOTICE OF DATA BREACH – PLEASE READ CAREFULLY**

Dear Neil H Levitt,

Perry Johnson & Associates, Inc. ("PJ&A," "we," or "us") is providing this letter to inform you of an event that may affect your personal health information. This letter provides details of the event, our response, and resources available to you to help protect your personal health information from possible misuse, should you feel it is appropriate to do so.

Who Is PJ&A and Why Did We Have Your Information? PJ&A serves as a vendor to Northwell Health, Inc. and its subsidiaries and affiliates (collectively, "Northwell"). PJ&A provides certain transcription and dictation services to Northwell. In order to perform these services, PJ&A receives personal health information regarding Northwell patients.

What Happened. PJ&A became aware of a data security incident impacting our systems on May 2, 2023. We immediately initiated an investigation and engaged a cybersecurity vendor to further provide support in connection with our investigation and secure against potential system vulnerabilities. We promptly implemented the cybersecurity vendor-recommended actions to prevent the further disclosure of data as we continued to investigate the situation. Through our investigation, we determined that the unauthorized access to our systems occurred between March 27, 2023 and May 2, 2023, and the unauthorized access to Northwell patient data specifically occurred between April 7, 2023 and April 19, 2023.

On July 21, 2023, PJ&A notified Northwell that an unauthorized party had accessed and downloaded certain files from our systems. PJ&A had preliminarily determined that Northwell data was impacted on May 22, 2023 and, by September 28, 2023, confirmed the scope of the Northwell data impacted.

What Information Was Involved. We have confirmed that certain files containing your personal health information were impacted by this incident. Specifically, the following information may have been impacted: your name, date of birth, address, medical record number, hospital account number, and clinical information such as the name of the treatment facility, the name of your healthcare providers, admission diagnosis, date(s) and time(s) of service, and files containing transcripts of operative reports, consult reports, history and physical exams, discharge summaries or progress notes, which may include the reason for your visit, your diagnoses, laboratory and diagnostic testing results, medical history including family medical history, surgical history, social history, medications, allergies, and/or other observational information.

What We Are Doing. We are committed to maintaining the privacy and security of your information and take this incident very seriously. PJ&A took, and will continue to take, appropriate steps to address this incident, including updating our systems to prevent incidents of this nature from occurring in the future. As soon as we

1489 W. Warm Springs Rd STE 110 | Henderson NV 89014 | (800) 803-6330 | www.pjats.com | info@pjats.com

B103450

-1-

1621531



K0005-L02